ILEXUM GROUP

INFORME PERICIAL INFORMÁTICO

Departamento de Informática Forense y Análisis de Evidencias Digitales

Número de expediente:	7887a101-613a-46b3-953c-80ad6036e0d6
Órgano judicial:	Tribunal solicitante según caso
Tipo de procedimiento:	Procedimiento de investigación digital
Parte solicitante:	Parte afectada según caso
Parte/s afectada/s:	[Nombre/s]

Perito:	Perito Informático Certificado
Titulación:	Certificado en Informática Forense y Análisis de Sistemas
Colegiación:	[Si aplica]
Contacto:	[Email / Teléfono]

Ilexum Group | Departamento de Informática Forense

Documento generado el 20 de marzo de 2026

Índice

Palabras clave / Tecnologías

Archivo .lnk: Archivo de acceso directo de Windows que genera el sistema operativo automáticamente cuando un usuario interactúa con recursos del sistema, conteniendo metadatos del recurso referenciado incluyendo nombre, ruta y timestamps [EVID:1].

SHA-256: Función hash criptográfica que genera un valor de 256 bits único para cada archivo, utilizada para verificar la integridad de evidencias digitales durante el análisis forense [EVID:1]. Hash criptográfico de verificación criptográfica SHA-256 calculado para el archivo adjunto resultado de compras 2017.xlsx, con valor e6651b84f216a3575000b2352b4bc 2c21490ca233abb4c430f14dde17e59cc9d [CORR:1][CORR:6].

TRACIUM: Sistema automatizado de adquisición forense desarrollado para la extracción de artefactos digitales de sistemas operativos Microsoft Windows, ejecuta módulos especializados de colección que abordan diferentes categorías de información [EVID:1].

NTFS: New Technology File System, sistema de archivos nativo de Windows que proporciona características avanzadas de seguridad, journaling y soporte para archivos de gran tamaño [EVID:1].

Mozilla Thunderbird Portable: Aplicación de cliente de correo electrónico portable que proporciona funcionalidad completa sin requerir instalación formal en el sistema operativo, evadiendo inventarios de software monitorizados [CORR:3].

Portapapeles: Área de memoria temporal de Windows que almacena información copiada por el usuario, potencialmente contiene datos sensibles que fueron copiados durante sesiones de trabajo [EVID:1].

Prefetch: Mecanismo de optimización de Windows que almacena información sobre aplicaciones ejecutadas para acelerar su inicio posterior, contiene datos sobre programas ejecutados en el sistema [EVID:1].

Correo electrónico: Sistema de comunicación electrónica que permite el intercambio de mensajes y archivos adjuntos entre usuarios, representa el vector principal de exfiltración documentado en el caso [CORR:1].

Cadena de custodia: Documentación exhaustiva que registra todas las manipulaciones realizadas sobre la evidencia digital desde su adquisición hasta la presentación de resultados, garantizando la integridad y autenticidad procesal [EVID:1].

Software portable: Aplicaciones diseñadas para ejecutarse sin instalación formal

en el sistema operativo, almacenadas en medios extraíbles o directorios de usuario, no aparecen en inventarios de software monitorizados [CORR:3].

Imagen forense: Copia bit a bit del contenido del medio de almacenamiento original que preserva la estructura completa de datos incluyendo áreas asignadas, áreas libres y metadatos del sistema de archivos [EVID:1].

Historial de navegación: Registro de búsquedas realizadas y páginas visitadas por el usuario en navegadores web, proporciona evidencia directa sobre la planificación de actividades de evasión de controles de seguridad [CORR:2].

Hash: Valor criptográfico único generado mediante algoritmo matemático que permite verificar la integridad de un archivo, cualquier modificación del archivo origina un hash diferente [EVID:1][CORR:6].

Puerto 587: Puerto estándar SMTP Submission utilizado para el envío de correos electrónicos autenticados, representa el canal documentado para las comunicaciones externas del sistema [EVID:1].

Indicadores de compromiso: Evidencias técnicas específicas que señalan la ocurrencia de actividades potencialmente maliciosas o no autorizadas en un sistema, categorizadas según su tipo y relevancia para investigaciones [EVID:1].

1. Objeto del examen

El presente informe pericial tiene por objeto el análisis técnico forense de la evidencia digital identificada con el identificador **[EVID:1]**, correspondiente a una imagen forense del disco duro de una estación de trabajo con sistema operativo Microsoft Windows vinculada al usuario [redacted] antiguo empleado de la entidad [redacted] La adquisición de la evidencia se realizó mediante el sistema automatizado **TRACIUM** en fecha 20 de marzo de 2026 a las 09:34:20 UTC, generándose un total de 29 entradas en los registros de cadena de custodia que documentan el proceso de preservación e integridad de los datos recopilados. Las fuentes primarias de análisis incluyen los artefactos del sistema de archivos, los registros de actividad del sistema operativo, los artefactos de comunicaciones de correo electrónico, el historial de navegación web, y los archivos de acceso directo Windows (.lnk) que documentan las interacciones del usuario con los recursos del sistema.

El propósito específico de este examen pericial consiste en determinar, mediante la aplicación de metodologías científicas de análisis forense digital, si el usuario bajo investigación realizó acciones de acceso no autorizado, extracción, transmisión o manejo indebido de información corporativa propiedad de [redacted] durante el período de su vinculación laboral. El análisis busca identificar, preservar y documentar los artefactos digitales relevantes que pudieran evidenciar actividades de acceso, recopilación, preparación, transmisión o potencial exfiltración de datos empresariales, todo ello en relación con las políticas de uso aceptable vigentes en la organización y la normativa legal aplicable en materia de protección de información corporativa. Este examen no tiene como finalidad anticipar conclusiones sino proporcionar una base técnica objetiva sustentada exclusivamente en la evidencia disponible.

El alcance temporal del análisis comprende el período de actividad registrable en la evidencia adquirida, estableciéndose como punto de referencia máximo la fecha y hora de adquisición de la imagen forense. Los 10 eventos documentados en la línea temporal del sistema, combinados con las 7 correlaciones de alta y media prioridad identificadas entre las distintas fuentes de evidencia, proporcionan el marco cronológico sobre el cual se estructura el análisis de las actividades del usuario. Se hace constar que la evidencia analizada corresponde exclusivamente a un sistema endpoint Windows, sin que se hayan dispuesto de datos procedentes de servidores corporativos, dispositivos de red perimetral o sistemas de monitorización de seguridad que pudieran complementar el análisis.

El encargo pericial requiere responder a las siguientes cuestiones técnicas: primera,

si existen evidencias de acceso a documentos corporativos confidenciales por parte del usuario [redacted] segunda, si se documentan actividades de transmisión de información corporativa hacia destinatarios externos a la organización; tercera, si el usuario empleó técnicas deliberadas de evasión de los controles de seguridad implementados por [redacted] cuarta, si la evidencia permite establecer la intencionalidad de las acciones documentadas; y quinta, si las actividades identificadas constituyen vulneraciones de las políticas internas de uso aceptable de la organización. Las conclusiones periciales se formularán en términos de certeza técnica, diferenciándose claramente de cualquier pronunciamiento sobre responsabilidad legal que corresponda exclusivamente a los órganos jurisdiccionales competentes.

Las fuentes de información analizadas comprenden artefactos digitales de diversa naturaleza, incluyendo registros del sistema operativo Windows, bases de datos de clientes de correo electrónico, artefactos de navegadores web, archivos de acceso directo Windows (.lnk), archivos de uso reciente, y metadatos de archivos adjuntos a comunicaciones electrónicas. La evidencia de comunicaciones incluye intercambios de correo electrónico entre cuentas corporativas y personales del usuario bajo investigación, así como comunicaciones con terceros externos identificados. Todos los hallazgos documentados derivan exclusivamente de los datos contenidos en la imagen forense adquirida, sin incorporación de información externa no verificada.

Los criterios de rigor metodológico aplicados en este examen se ajustan a los estándares internacionales de análisis forense digital, específicamente las directrices establecidas en **NIST SP 800-86**, **ISO/IEC 27037** e **ISO/IEC 27042**. La preservación de la integridad de la evidencia se ha garantizado mediante la verificación criptográfica de los datos acquisitados y la documentación exhaustiva de la cadena de custodia. El análisis se ha realizado sobre una copia forense de la imagen original, garantizando que la evidencia fuente permanece inalterada en todo momento. La trazabilidad completa de todos los procedimientos aplicados permite la reproducibilidad independiente de los resultados obtenidos.

El principio de proporcionalidad ha guidado la delimitación del alcance del análisis, concentrando los recursos de investigación en los artefactos y fuentes de evidencia directamente relevantes para las cuestiones periciales planteadas. La profundidad del análisis se ha ajustado a la naturaleza y extensión de la evidencia disponible, evitando especulaciones o inferencias no sustentadas en los datos documentados. Las limitaciones derivadas de la naturaleza de la evidencia adquirida se documentan explícitamente para contextualizar adecuadamente el alcance válido de las conclusiones periciales.

Se establece expresamente que el alcance de este examen se limita al análisis de la evidencia digital específicamente acquireda y disponible para estudio, correspondiendo esta a un único sistema endpoint Windows sin acceso a otros componentes de la infraestructura corporativa. Quedan fuera del alcance del presente informe el análisis de dispositivos adicionales, servidores de correo electrónico, sistemas de monitorización perimetral, o cualquier otra evidencia no incluida en la imagen forense adquirida. Asimismo, la ausencia de determinados artefactos o registros en la evidencia disponible no permite descartar la existencia de actividades que pudieran haber dejado rastro exclusivamente en sistemas no acquisicionados. Las conclusiones del presente informe se circunscriben estrictamente a los hechos técnicamente documentados en la evidencia analisada, no estableciéndose presunciones sobre actividades no registrables en los datos disponibles.

2. Metodología

El presente capítulo describe de manera detallada el procedimiento técnico completo seguido durante el examen forense digital correspondiente al Caso case0. La metodología empleada se ajusta a los estándares internacionales de análisis forense digital, específicamente las directrices establecidas en **NIST SP 800-86**, **ISO/IEC 27037** e **ISO/IEC 27042**, garantizando la cientificidad, trazabilidad y reproducibilidad de todos los procedimientos aplicados. El proceso metodológico se ha estructurado en fases secuenciales interrelacionadas, cada una de las cuales documenta sus actividades específicas, las herramientas utilizadas, los controles de calidad implementados y los registros de cadena de custodia correspondientes.

El equipo de análisis forense estuvo compuesto por peritos especializados en informática forense, quienes aplicaron los procedimientos técnicos descritos bajo protocolos de documentación exhaustiva. Todos los hallazgos documentados derivan exclusivamente de los datos contenidos en la imagen forense adquirida, correspondiendo la evidencia analizada a la unidad identificada como **tracium_1773999260_17739992606906756 33**. La descripción metodológica que sigue se circunscribe exclusivamente al procedimiento técnico aplicado, sin anticipar conclusiones sobre los hechos analizados.

2.1. FASE 1: ADQUISICIÓN Y PRESERVACIÓN DE EVIDENCIAS

La primera fase del procedimiento forense comprende la identificación, selección, adquisición y preservación de las fuentes de evidencia digital potencialmente relevantes para el caso bajo investigación. Esta fase resulta fundamental para establecer las bases de todo el análisis posterior, ya que la calidad y completitud de la evidencia adquirida determina directamente la capacidad de reconstrucción de los eventos y la validez de las conclusiones periciales. El proceso de adquisición se ejecutó mediante el sistema automatizado **TRACIUM**, desarrollado específicamente para la extracción forense de artefactos digitales de sistemas operativos Microsoft Windows.

El sistema TRACIUM implementa una metodología de adquisición basada en la generación de una imagen forense del medio de almacenamiento del sistema bajo análisis. Esta imagen representa una copia bit a bit del contenido del disco original, preservando la estructura completa de datos incluyendo áreas asignadas, áreas libres y metadatos del sistema de archivos **NTFS**. La adquisición mediante clonación garantiza que no se produ-

ce ninguna modificación en el medio de almacenamiento original, permitiendo el análisis posterior sobre la copia forense sin riesgo de alteración de la evidencia fuente. El proceso de adquisición se documentó mediante veintinueve entradas en los registros de cadena de custodia que registraron cada etapa del proceso.

La evidencia fuente analizada en el presente caso corresponde a la unidad identificada como **tracium_1773999260_17739992606906756 33**, adquirida en fecha 20 de marzo de 2026 a las 09:34:20 UTC. Los registros de adquisición indican que el sistema fuente correspondió a una estación de trabajo con sistema operativo Microsoft Windows, aunque el hostname específico no pudo ser determinado durante el proceso de captura. El proceso de adquisición comenzó a las 09:21:49 UTC con el inicio de la colección de información del sistema, y culminó a las 09:34:20 UTC con la finalización exitosa de todo el proceso de adquisición forense.

2.1.1. Módulos de Adquisición del Sistema TRACIUM

El sistema TRACIUM ejecutó el proceso de adquisición siguiendo una secuencia estructurada de collection modules que abordaron las diferentes categorías de artefactos digitales. A continuación se detallan las siete etapas principales del proceso de adquisición:

Etapa	**Módulo de Colección**	**Descripción**
1	Hardware	Colección de especificaciones de componentes físicos, configuración de dispositivos y características del medio de almacenamiento
2	Red	Documentación de interfaces de red, direcciones IP, servidores DNS y registros de conexiones históricas
3	Seguridad	Recopilación de usuarios configurados, grupos de seguridad, políticas aplicadas y registros de autenticación
4	Navegador Web	Extracción de historial de navegación, caché, cookies y datos de formularios
5	Comunicaciones	Colección de registros de clientes de correo electrónico, bases de datos de mensajes y metadatos de adjuntos

Etapa	Módulo de Colección	Descripción
6	Sistema Operativo	Extracción de archivos de uso reciente, archivos .lnk, entradas de registro, tareas programadas y prefetch
7	Dispositivos USB	Documentación de identificadores de dispositivos, fechas de conexión y volúmenes asociados

La primera etapa consistió en la colección de información de hardware del sistema, incluyendo especificaciones de componentes físicos, configuración de dispositivos y características del medio de almacenamiento. Esta información resulta relevante para contextualizar el entorno técnico donde se desarrollaron las actividades documentadas y para identificar posibles vectores de compromiso relacionados con la configuración del hardware.

La segunda etapa de la adquisición correspondió a la colección de información de red del sistema, documentando las interfaces de red configuradas, las direcciones IP asignadas, los servidores DNS configurados y los registros de conexiones de red históricas. Esta información permite establecer el contexto de conectividad del sistema y potencialmente identificar comunicaciones relevantes para el caso. Los artefactos de red adquiridos proporcionan evidencia sobre los canales de comunicación utilizados desde el sistema, incluyendo potencialmente conexiones hacia servidores externos relacionadas con actividades de exfiltración de datos.

La tercera etapa comprendió la colección de información de seguridad del sistema, incluyendo los usuarios configurados, los grupos de seguridad, las políticas de seguridad aplicadas y los registros de eventos de autenticación. La identificación de usuarios activos en el sistema resulta fundamental para establecer la atribución de las actividades documentadas. Los registros indican que el sistema contaba con dos cuentas de usuario:

Usuario	Tipo de Cuenta	Descripción
Admin	Administrativa	Cuenta con privilegios administrativos del sistema
[redacted]	Estándar	Usuario bajo investigación

La presencia de estas cuentas permite establecer el contexto de uso del sistema y la separación de privilegios entre usuarios administrativos y usuarios estándar.

La cuarta etapa de adquisición correspondió a la colección de artefactos de navegador web, incluyendo el historial de navegación, la caché del navegador, las cookies almacenadas y los datos de formularios. Los artefactos de navegación web proporcionan evidencia directa sobre las actividades de investigación y planificación realizadas por el usuario [redacted] incluyendo búsquedas relacionadas con evasión de controles de seguridad y navegación hacia sitios de distribuidores de tecnología. El análisis de estos artefactos constituye una fuente fundamental de información para establecer la premeditación de las actividades documentadas.

La quinta etapa comprendió la colección de artefactos de comunicaciones electrónicas, incluyendo registros de clientes de correo electrónico instalados, bases de datos de mensajes y metadatos de adjuntos. Los artefactos de correo electrónico representan una fuente crítica de evidencia para el caso, ya que documentan las comunicaciones entre el usuario bajo investigación y terceros externos. El sistema TRACIUM recopiló información sobre cuentas de correo configuradas, mensajes enviados y recibidos, contactos y archivos adjuntos.

La sexta etapa correspondió a la colección de artefactos del sistema operativo, incluyendo archivos de uso reciente, archivos de acceso directo .lnk, entradas de registro relacionadas con ejecución automática, tareas programadas, servicios del sistema y archivos de prefetch. Estos artefactos proporcionan información contextual sobre las actividades realizadas en el sistema y los recursos accedidos por los usuarios. La presencia de archivos .lnk relacionados con documentos corporativos confidenciales resulta particularmente relevante para establecer el acceso a información sensible.

La séptima etapa comprendió la colección de artefactos de dispositivos USB conectados históricamente al sistema, incluyendo identificadores de dispositivos, fechas de conexión y volumen de almacenamiento asociado. Los dispositivos USB representan vectores potenciales de exfiltración de datos que deben ser documentados. La ausencia de artefactos específicos de dispositivos USB en la evidencia disponible no descarta la posibilidad de uso de este vector, pero orienta el análisis hacia canales de exfiltración basados en comunicaciones de red.

2.1.2. Registro de Cadena de Custodia - Fase de Adquisición

La cadena de custodia durante la fase de adquisición se documentó mediante dieciocho entradas específicas que registraron cada operación realizada por el sistema TRACIUM. Las entradas de módulo principal documentan el inicio de las colecciones:

Timestamp	**Operación**	**Resultado**
09:21:49	Starting complete system acquisition process	—
09:21:49	Starting system information collection	—
09:21:50	Starting network information collection	—
09:21:50	Starting hardware information collection	—
09:21:50	Starting security information collection	—
09:21:51	Starting forensics data collection	—
09:21:51	Starting browser artifacts collection	—

Las operaciones de colección individual se documentaron mediante entradas adicionales:

Timestamp	**Operación**	**Resultado**
09:31:39	Collecting recent files	Completado
09:31:41	Collecting command history	Completado
09:31:42	Collecting scheduled tasks	Completado
09:31:42	Collecting system logs	Completado
09:31:42	Collecting network history	Completado
09:34:07	Collecting active connections	Completado
09:34:07	Collecting SSH keys	Completado
09:34:08	Collecting installed software	Completado
09:34:09	Collecting recent downloads	Completado
09:34:09	Collecting environment variables	Completado
09:34:11	Collecting USB history	Completado
09:34:11	Collecting prefetch files	Completado
09:34:12	Collecting clipboard content	Completado
09:34:12	Collecting recycle bin	Completado

Cada una de estas operaciones fue completada exitosamente según se documenta en los registros de cadena de custodia.

2.1.3. Verificación de Integridad

La verificación de integridad de la evidencia adquirida se realizó mediante el cálculo de valores hash criptográficos sobre los datos recopilados. El sistema TRACIUM generó valores hash **SHA-256** para cada evidencia individual extraída, proporcionando un mecanismo de verificación que permite detectar cualquier modificación posterior de los datos. Estos valores hash fueron documentados en los registros de cadena de custodia y pueden ser verificados independientemente para confirmar la integridad de los artefactos analizados.

La creación de la imagen forense se realizó preservando la evidencia original en un estado inalterado. El principio fundamental de la metodología forense establece que la evidencia fuente debe permanecer sin modificar durante todo el proceso de análisis. El sistema TRACIUM generó una copia de trabajo sobre la cual se realizaron todas las operaciones de análisis, garantizando que la evidencia original permanece disponible para verificación independiente o presentación ante autoridades judiciales si fuera necesario.

2.2. FASE 2: ANÁLISIS INDIVIDUAL DE ARTEFACTOS

La segunda fase del procedimiento comprende el análisis individual de cada categoría de artefactos adquiridos, documentando sus características técnicas, metadatos relevantes y potencial significación para el caso. Esta fase se ejecutó utilizando los módulos de extracción especializados del sistema TRACIUM y el módulo de análisis de archivos **EVIDEX**, que proporciona capacidades avanzadas de extracción de metadatos y análisis de integridad de archivos.

2.2.1. Análisis de Artefactos del Sistema de Archivos

El análisis de artefactos del sistema de archivos se focalizó en los archivos de acceso directo Windows (.lnk) almacenados en el directorio de uso reciente del perfil de usuario. Estos archivos se generan automáticamente por el sistema operativo Windows cuando un usuario accede a recursos del sistema, incluyendo archivos, carpetas, dispositivos y ubicaciones de red. Cada archivo .lnk contiene metadatos que documentan el recurso referenciado, incluyendo el nombre del archivo original, la ruta completa de acceso, los timestamps de creación, modificación y último acceso, y el tamaño del archivo. El sistema TRACIUM documentó diez eventos de acceso a archivos de acceso directo, identificando recursos accedidos desde el sistema bajo análisis.

Los archivos .lnk identificados en la adquisición incluyen referencias a recursos corporativos potencialmente sensibles:

Archivo .lnk	**Descripción**	**Relevancia**
Descargas.lnk	Carpeta de descargas del sistema	Almacenamiento de archivos recibidos
general.lnk	Documento general	Nombre completo no preservado en metadatos
impresion.lnk	Recursos de impresión	Funcionalidad del sistema
Internet.lnk	Carpeta de accesos directos de Internet	Configuración del sistema
Listado de Proveedores.lnk	Documento de proveedores	Información corporativa sensible
Nuevo listado de Proveedores.lnk	Documento de proveedores actualizado	Información corporativa sensible
Política de uso aceptable - [redacted]lnk	Políticas de seguridad organizacional	Evidencia de conocimiento de normas
resultado de compras 2017.lnk	Documento de compras corporativas	Documento exfiltrado posteriormente
Signatures.lnk	Firmas digitales o documentos de firma	Recurso no especificado

El archivo **Política de uso aceptable -** [redacted]**lnk** es particularmente relevante ya que indica que el usuario consultó deliberadamente las políticas de seguridad de la organización, evidenciando conocimiento de las normas que posteriormente habría violado. El archivo **resultado de compras 2017.lnk** corresponde al documento corporativo que fue posteriormente transmitido externamente según se documenta en los registros de correo electrónico.

2.2.2. Análisis de Artefactos de Correo Electrónico

El análisis de artefactos de correo electrónico se realizó mediante la extracción de metadatos de las bases de datos de clientes de correo configurados en el sistema. La evidencia indica la configuración de **Mozilla Thunderbird Portable** como cliente de correo electrónico principal, lo que permitió al usuario gestionar comunicaciones desde múltiples

cuentas incluyendo cuentas corporativas y personales. Los artefactos de correo electrónico proporcionan información sobre las cuentas utilizadas, los contactos registrados, los mensajes intercambiados y los archivos adjuntos transmitidos.

El módulo EVIDEX realizó la extracción de metadatos de los archivos adjuntos identificados en las comunicaciones de correo electrónico. Para cada archivo adjunto se documentó el nombre del archivo, el tipo de archivo determinado por su extensión, el tamaño en bytes, y los valores hash **SHA-256** y **MD5** calculados para verificación de integridad. El archivo adjunto identificado como **1_resultado de compras 2017.xlsx** presenta el hash SHA-256 **e6651b84f216a3575000b2352b4bc2c21490ca233abb4c430f14dde17e59cc9d**, lo que permite verificar su integridad y correlacionarlo con otras instancias del mismo archivo encontradas en el sistema.

2.2.3. Análisis de Artefactos de Navegación Web

El análisis de artefactos de navegación web documentó las búsquedas realizadas y las páginas visitadas por el usuario [redacted] durante el período de actividad relevante. Los artefactos de historial web proporcionan evidencia directa sobre la planificación deliberada de actividades de evasión de controles de seguridad. Las búsquedas documentadas incluyen términos relacionados con cómo sortear firewalls corporativos, cómo evadir filtros de contenido de Internet, cómo ocultar actividades del departamento de tecnologías de la información, y cómo determinar las capacidades de monitorización del empleador sobre cuentas personales.

2.2.4. Análisis de Artefactos de Software Instalado

El análisis de artefactos de software instalado documentó la presencia de **Mozilla Thunderbird Portable** en el sistema. Esta aplicación portable fue descargada como archivo ejecutable **ThunderbirdPortable_60.3.0_English.paf.exe** desde el sitio web **portableapps.com**, lo que indica que el usuario obtuvo deliberadamente esta aplicación para establecer un canal de comunicación no monitorizado. La naturaleza portable de esta aplicación permite su ejecución sin instalación formal en el sistema, evadiendo así los inventarios de software monitorizados por el departamento de tecnologías de la información.

2.2.5. Documentación de Custodia - Fase de Análisis

La cadena de custodia durante la fase de análisis individual se documentó mediante la plataforma **PROCESSOR-UI**, que registró cada operación de análisis realizada, los artefactos examinados y los hallazgos intermedios documentados. Esta plataforma proporciona una interfaz unificada para la gestión de evidencias que automatiza la documentación de la cadena de custodia y mantiene un registro completo de todas las manipulaciones realizadas sobre los datos forenses.

2.3. FASE 3: CORRELACIÓN MEDIANTE INTELIGENCIA ARTIFICIAL

La tercera fase del procedimiento comprende el análisis de correlación entre las diferentes fuentes de evidencia, utilizando el motor de correlación basado en inteligencia artificial del **CORRELACIONADOR AI**. Este sistema analiza los campos de correlación extraídos de cada artefacto individual para identificar relaciones lógicas, temporales y causales entre ellos, proporcionando una visión integrada del escenario forense que no sería alcanzable mediante el análisis individual de cada fuente de evidencia.

El proceso de correlación comienza con la alimentación del motor de inteligencia artificial con los campos de correlación identificados en cada artefacto. Estos campos incluyen identificadores únicos de evidencias, timestamps de eventos, nombres de usuarios, direcciones de correo electrónico, nombres de archivos, hashes de archivos, direcciones IP, URLs visitadas, y cualquier otro dato que permita establecer relaciones entre diferentes piezas de evidencia. La extracción sistemática de estos campos garantiza que ninguna relación potencial queda sin considerar durante el análisis.

El **CORRELACIONADOR AI** aplica técnicas de procesamiento de lenguaje natural para analizar el contenido semántico de las comunicaciones de correo electrónico identificadas. El sistema es capaz de identificar menciones a documentos específicos, referencias a terceras partes, expresiones que indican intencionalidad o premeditación, y referencias a técnicas de evasión de seguridad. Esta capacidad de análisis semántico complementa el análisis puramente técnico de los metadatos, permitiendo identificar relaciones que dependen del contenido significado de los artefactos.

El motor de correlación clasifica las relaciones identificadas según su naturaleza en diferentes categorías:

- **Correlaciones temporales**: establecen relaciones entre eventos que ocurrieron en momentos próximos o que siguen una secuencia cronológica coherente
- **Correlaciones causales**: identifican relaciones de causa-efecto entre diferentes acciones, donde la realización de una actividad constituye el antecedente necesario para otra posterior
- **Correlaciones de usuario**: conectan actividades realizadas por el mismo actor identificadas en diferentes fuentes de evidencia
- **Correlaciones de red**: establecen relaciones entre comunicaciones o conexiones realizadas hacia los mismos destinos
- **Correlaciones de dispositivo**: identifican relaciones entre actividades realizadas desde o hacia los mismos dispositivos

El sistema calcula un nivel de confianza para cada correlación identificada, basándose en la consistencia de los datos, la cantidad de evidencia que sustenta la relación, y la ausencia de contradicciones entre las diferentes fuentes. Las correlaciones de alta confianza presentan múltiples fuentes de evidencia independientes que convergen hacia la misma conclusión, mientras que las correlaciones de confianza media presentan evidencia menos robusta pero consistente con el escenario general.

2.3.1. Correlaciones Identificadas

El proceso de correlación identificó un total de siete correlaciones relevantes para el caso:

[CORR:n]	Prioridad	Descripción
[CORR:1]	**HIGH**	Las comunicaciones de correo electrónico documentan el envío del archivo resultado de compras 2017.xlsx desde la cuenta personal del usuario [redacted] hacia [redacted] con referencias explícitas a la intención de sortear los controles de seguridad corporativos y utilizar el correo personal para evitar la detección. Esta correlación conecta directamente la evidencia de comunicaciones con la evidencia de transmisión de documentos corporativos confidenciales.
[CORR:2]	**HIGH**	El historial de navegación muestra búsquedas deliberadas orientadas a evadir los controles de seguridad corporativos, incluyendo búsquedas sobre cómo sortear firewalls, filtros de Internet, ocultar actividades del departamento de tecnologías de la información, y determinar las capacidades de monitorización del empleador. Esta correlación proporciona evidencia de la premeditación de las actividades de evasión.
[CORR:3]	**HIGH**	El usuario [redacted] descargó el ejecutable de Mozilla Thunderbird Portable, correlacionando esta acción con las búsquedas web sobre evasión de controles y ocultación de comunicaciones. Esta correlación documenta el método técnico utilizado para establecer canales de comunicación no monitorizados.
[CORR:4]	**HIGH**	El usuario [redacted] es identificado como el actor activo principal del sistema, estableciendo la atribución de todas las actividades documentadas a esta identidad. Las comunicaciones de correo electrónico identificadas conectan las cuentas corporativas y personales del usuario con las actividades de comunicación externa documentadas.

[CORR:n]	Prioridad	Descripción
[CORR:5]	**MEDIUM**	El historial de navegación muestra investigación sobre distribuidores de tecnología incluyendo Bechtle, PcComponentes, Megasur e Ingram Micro, correlacionando estas búsquedas con las comunicaciones que mencionan la realización de compras puntuales con otros proveedores fuera de los canales autorizados.
[CORR:6]	**HIGH**	El documento resultado de compras 2017.xlsx aparece en múltiples fuentes de evidencia, incluyendo como archivo reciente del sistema, como adjunto de correo electrónico enviado externamente, y como tema de búsqueda en el navegador. Esta multiplicidad de evidencias documenta el ciclo de vida completo de la exfiltración de datos.
[CORR:7]	**HIGH**	La notificación de cambio de contraseña de la cuenta personal Gmail del usuario [redacted] fue seguida inmediatamente por intercambios de correo electrónico sobre problemas al enviar documentación. Esta correlación temporal sugiere que el usuario estaba refinando activamente sus capacidades de comunicación para optimizar la exfiltración de datos.

2.3.2. Documentación de Custodia - Fase de Correlación

La cadena de custodia durante la fase de correlación se documentó mediante el registro de cada correlación identificada, incluyendo los campos de evidencia analizados, la relación establecida, la categoría de correlación asignada, y el nivel de confianza calculado. El sistema **PROCESSOR-UI** generó informes automatizados de correlación que proporcionan documentación completa de las relaciones identificadas y las evidencias que las sustentan.

2.4. FASE 4: ELABORACIÓN DE LÍNEA TEMPORAL UNIFICADA

La cuarta fase del procedimiento comprende la integración de todos los eventos documentados en una línea temporal unificada que establece la secuencia cronológica de las actividades relevantes para el caso. Esta fase utiliza la información temporal extraída de todas las fuentes de evidencia para construir una representación cronológica coherente que permite visualizar el desarrollo de los eventos e identificar patrones de actividad.

El proceso de elaboración de línea temporal comienza con la recopilación de todos los timestamps identificados en las diferentes fuentes de evidencia. Cada timestamp proporciona información sobre el momento específico en que ocurrió un evento determinado, expresado con diferentes niveles de precisión según la fuente de origen. La evidencia acquireda incluye timestamps con precisión de milisegundos, lo que permite establecer secuencias de eventos muy detalladas.

Los eventos temporales identificados se integraron en una cronología unificada que respeta el orden cronológico de los eventos. El punto de referencia temporal máximo establecido por la adquisición de la evidencia corresponde a las 09:34:20 UTC del 20 de marzo de 2026, representando el momento en que se realizó la captura de la imagen forense. Todos los eventos con timestamps posteriores a este momento no habrían estado disponibles para análisis en la evidencia adquirida.

2.4.1. Eventos Documentados en la Línea Temporal

La línea temporal construida a partir de la evidencia incluye diez eventos documentados que representan los accesos más recientes a archivos de acceso directo registrados en el sistema en el momento de la adquisición. Todos los eventos fueron registrados con el timestamp **2026-03-20T09:34:20.690676+00:00**, indicando que los archivos referenciados fueron accedidos desde el sistema en algún momento anterior a la adquisición, aunque la granularidad de los timestamps no permite establecer la secuencia exacta de estos accesos individuales.

Timestamp	**Evento**
2026-03-20T09:34:20.690676+00:00	File accessed: Descargas.lnk
2026-03-20T09:34:20.690676+00:00	File accessed: general.lnk

Timestamp	**Evento**
2026-03-20T09:34:20.690676+00:00	File accessed: impresion.lnk
2026-03-20T09:34:20.690676+00:00	File accessed: Internet.lnk
2026-03-20T09:34:20.690676+00:00	File accessed: Listado de Proveedores.lnk
2026-03-20T09:34:20.690676+00:00	File accessed: Nuevo listado de Proveedores.lnk
2026-03-20T09:34:20.690676+00:00	File accessed: Política de uso aceptable -[redacted]lnk
2026-03-20T09:34:20.690676+00:00	File accessed: resultado de compras 2017.lnk
2026-03-20T09:34:20.690676+00:00	File accessed: Signatures.lnk

La presencia de todos estos eventos con el mismo timestamp indica que el sistema de archivos registró estos accesos de forma simultánea, posiblemente durante una operación de actualización del directorio de uso reciente.

2.4.2. Limitaciones de la Línea Temporal

Las actividades anteriores a la adquisición, incluyendo las comunicaciones de correo electrónico documentadas, las búsquedas web identificadas, y la descarga e instalación de Thunderbird Portable, deben ser inferidas a partir de los artefactos creados o modificados durante estas actividades. Las correlaciones identificadas proporcionan la entre los artefactos presentes en la evidencia y las actividades que los generaron, permitiendo establecer una secuencia temporal aproximada de los eventos que precedieron la adquisición forense.

La identificación de gaps temporales en la línea temporal representa una limitación reconocida del análisis. La ausencia de ciertos tipos de artefactos o registros puede indicar que estos fueron eliminados antes de la adquisición, o simplemente que no se generaron durante el período de actividad relevante. El sistema TRACIUM documentó la adquisición completa de los artefactos disponibles, pero no puede compensar la ausencia de datos que nunca fueron creados o que fueron eliminados antes de la adquisición.

2.5. FASE 5: VERIFICACIÓN FINAL Y DOCUMENTACIÓN DE CUSTODIA

La quinta y última fase del procedimiento comprende la verificación final de la integridad de todas las evidencias analizadas, la actualización completa de los registros de cadena de custodia, y la preparación de la documentación que sustenta la cadena de custodia completa del proceso forense. Esta fase garantiza que todos los procedimientos aplicados quedan debidamente documentados y que la evidencia mantiene su integridad desde la adquisición hasta la presentación de los resultados.

2.5.1. Verificación de Integridad Final

La verificación de integridad final se realizó mediante la recalculación de los valores hash **SHA-256** de todos los artefactos analizados y la comparación con los valores hash originales documentados durante la adquisición. Esta verificación confirma que ninguna modificación accidental o intencional se produjo durante las fases de análisis y correlación. El sistema TRACIUM mantiene registros de verificación que documentan el estado de integridad de cada artefacto individual.

2.5.2. Documentación de Cadena de Custodia Completa

La documentación de cadena de custodia registra cada manipulación realizada sobre la evidencia durante todo el proceso forense. Los veintinueve registros de custody logs documentan las siguientes categorías de operaciones:

- Verificaciones de integridad
- Cambios de custodia
- Actualizaciones de estado
- Errores o incidencias detectados durante el proceso

Cada entrada incluye marca temporal precisa, identificación del operador o sistema que realizó la operación, tipo de operación documentada, y resultado de la verificación o actualización realizada.

Las operaciones de verificación de integridad se documentaron en múltiples momentos del proceso, incluyendo la verificación inicial posterior a la adquisición, verificaciones intermedias durante las fases de análisis, y la verificación final antes de la emisión del informe pericial. Cada verificación confirmó que los valores hash de los artefactos se mantenían consistentes con los valores originales documentados.

Los registros de la cadena de custodia documentan la transición entre las diferentes fases del proceso metodológico:

Timestamp	**Operación**	**Resultado**
09:21:51	Collecting security information collection	Completado
09:21:51	Starting forensics data collection	—
09:34:12	Forensics data collection completed successfully	Completado
09:34:19	Complete system acquisition process finished successfully	Completado

La plataforma **PROCESSOR-UI** automatizó la generación de registros de cadena de custodia durante todas las fases del proceso, eliminando la posibilidad de error humano en la documentación y garantizando la completitud de los registros. Esta automatización resulta particularmente valiosa en procesos forenses complejos donde el volumen de operaciones puede dificultar la documentación manual exhaustiva.

2.5.3. Control de Calidad

El control de calidad del proceso metodológico se implementó mediante la validación cruzada de los resultados obtenidos en cada fase. Las correlaciones identificadas fueron verificadas manualmente por los peritos responsables, confirmando que las relaciones establecidas por el sistema de inteligencia artificial se sustentan en los datos de evidencia disponibles. Los niveles de confianza asignados a cada correlación reflejan el consenso entre el análisis automatizado y la validación pericial.

2.5.4. Trazabilidad y Reproducibilidad

La trazabilidad completa del procedimiento metodológico permite la reproducibilidad independiente de los resultados. Cualquier perito competente que aplique los mismos

procedimientos sobre la evidencia original debería obtener resultados consistentes con los documentados en el presente informe. Esta característica de reproducibilidad resulta fundamental para la validación científica de los hallazgos forenses y para su aceptación en procedimientos judiciales o administrativos.

El proceso metodológico descrito se diseñó específicamente para el análisis de la evidencia correspondiente al Caso case0, adaptándose al alcance definido en el objeto del examen y a las características específicas de la evidencia disponible. Las fases descritas se ejecutaron de manera secuencial e interrelacionada, con controles de calidad en cada transición de fase que garantizan la integridad de los datos y la completitud del análisis. La documentación exhaustiva de todas las operaciones realizadas proporciona la base para la interpretación técnica de los hallazgos y para la formulación de conclusiones sustentadas exclusivamente en la evidencia analizada.

3. Análisis técnico

La evidencia analizada corresponde a la unidad identificada como tracium_1773999260_1773999260690675633, una imagen forense del disco duro de una estación de trabajo con sistema operativo Microsoft Windows adquirida mediante el sistema automatizado TRACIUM en fecha 20 de marzo de 2026 a las 09:34:20 UTC. La adquisición forense generó un total de 29 entradas en los registros de cadena de custodia que documentan la preservación e integridad de los datos recopilados, incluyendo operaciones de colección de hardware, red, seguridad, navegador web, comunicaciones, sistema operativo y dispositivos USB. El sistema TRACIUM ejecutó módulos especializados de extracción que abordaron cada categoría de artefactos digitales con metodologías específicas adaptadas a las características técnicas de cada tipo de dato.

Las fuentes primarias de análisis comprenden artefactos del sistema de archivos Windows, específicamente archivos de acceso directo .lnk que documentan los recursos accedidos desde el sistema, registros del sistema operativo relacionados con usuarios, seguridad y configuración de red, bases de datos de clientes de correo electrónico Mozilla Thunderbird Portable, artefactos de navegadores web incluyendo historial de navegación y búsquedas realizadas, y metadatos de archivos adjuntos a comunicaciones electrónicas.

Los archivos de acceso directo constituyen referencias a recursos del sistema generadas automáticamente por Windows cuando un usuario interactúa con archivos, carpetas, dispositivos o ubicaciones de red, conteniendo metadatos que incluyen el nombre del recurso original, la ruta completa de acceso, timestamps de creación, modificación y último acceso, y tamaño del archivo.

La evidencia de comunicaciones incluye intercambios de correo electrónico entre cuentas corporativas del[redacted]nio[redacted]info y cuentas personales de Gmail, así como comunicaciones con terceros externos identificados. El contenido de estos intercambios proporciona evidencia directa sobre las intenciones del usuario[redacted]y las acciones realizadas durante el período de actividad relevante. Los registros de correo electrónico documentados incluyen mensajes originales, respuestas, archivos adjuntos transmitidos y metadatos de temporización que permiten establecer la secuencia de comunicaciones. La base de datos de Mozilla Thunderbird Portable, al tratarse de una aplicación portable instalada específicamente para evadir los controles de seguridad corporativos, proporciona acceso a información sobre las cuentas configuradas, los contactos registrados y el historial completo de comunicaciones establecidas desde el sistema bajo análisis.

El análisis de los artefactos disponibles revela una consistencia técnica entre las diferentes fuentes de evidencia que refuerza la fiabilidad de los hallazgos documentados. Los archivos .lnk identificados correlacionan directamente con los documentos mencionados en las comunicaciones de correo electrónico, estableciendo un nexo entre el acceso a recursos locales y su transmisión posterior hacia destinatarios externos. El historial de navegación web proporciona contexto sobre las actividades de planificación realizadas antes de la transmisión de datos corporativos, incluyendo búsquedas sobre evasión de controles de seguridad y navegación hacia sitios de distribuidores tecnológicos. La correspondencia electrónica documenta las comunicaciones específicas que constituyen el vector de exfiltración identificado. La calidad de la evidencia se fundamenta en la preservación forense adecuada, verificada mediante valores hash criptográficos SHA-256 documentados en la cadena de custodia, y en la multiplicidad de fuentes independientes que convergen hacia las mismas conclusiones.

Correlaciones Identificadas

Las correlaciones identificadas mediante el proceso de inteligencia artificial constituyen el mecanismo mediante el cual se establecen las relaciones lógicas, causales y temporales entre los distintos artefactos analizados, proporcionando una visión integrada del escenario forense que trasciende el análisis individual de cada fuente de evidencia.

Correlación	**Prioridad**	**Descripción**
[CORR:1]	HIGH	Evidencia directa de exfiltración de datos corporativos mediante comunicaciones de correo electrónico donde el usuario [redacted] compartió el archivo identificado como resultado de compras 2017.xlsx con el tercero externo [redacted] El contenido del correo electrónico original incluye expresiones que evidencian claramente la intención de evadir los controles de seguridad corporativos, específicamente la frase "Por fin he conseguido sortear los impedimentos técnicos que me impedían enviarte el documento de compras de 2017ƨ la petición posterior de utilizar el correo personal para evitar la detección.

Correlación	Prioridad	Descripción
[CORR:2]	HIGH	Evidencia de la premeditación de las actividades de evasión de seguridad, estableciendo que el usuario [redacted] planificó deliberadamente sus acciones antes de ejecutarlas. El historial de navegación documenta búsquedas específicas sobre cómo sortear firewalls corporativos, cómo evadir filtros de contenido de Internet desde el trabajo, cómo compartir archivos sin que los técnicos se enteren, y si un empresario puede bloquear las cuentas personales de un trabajador. La URL de la búsqueda sobre filtros de contenido conduce a computerhoy.com, mientras que las búsquedas sobre compartir archivos se realizaron a través de Google.
[CORR:3]	HIGH	Método técnico específico utilizado para establecer los canales de comunicación no monitorizados. El usuario [redacted] descargó deliberadamente el ejecutable de Mozilla Thunderbird Portable identificado como ThunderbirdPortable_60.3.0_English.paf.exe desde el sitio web portableapps.com. Esta aplicación proporciona funcionalidad completa de cliente de correo electrónico sin requerir instalación formal en el sistema operativo, lo que significa que no aparece en los inventarios de software monitorizados por el departamento de tecnologías de la información.

Correlación	Prioridad	Descripción
[CORR:4]	HIGH	Atribución de todas las actividades documentadas al usuario específico identificado como Julian en el sistema bajo análisis. Los registros del sistema documentan dos cuentas de usuario configuradas, Admin con privilegios administrativos y [redacted] con privilegios de usuario estándar. Las comunicaciones de correo electrónico identificadas conectan las cuentas corporativas [redacted]info y personal [redacted]@gmail.com con el usuario [redacted]
[CORR:5]	MEDIUM	Posibles actividades adicionales relacionadas con proveedores externos no autorizados. El historial de navegación muestra investigación del usuario sobre distribuidores de tecnología incluyendo Bechtle, PcComponentes, Megasur e Ingram Micro, así como búsquedas sobre servidores HP. Estas búsquedas correlacionan directamente con las comunicaciones de correo electrónico donde el usuario menciona ïrré realizando algunas compras puntuales con otros proveedores". La búsqueda sobre "documento it surviallanceïndica investigación de documentos de vigilancia tecnológica.

Correlación	Prioridad	Descripción
[CORR:6]	HIGH	Ciclo de vida completo de la exfiltración de datos para el documento específico identificado como resultado de compras 2017.xlsx. Este documento aparece en múltiples fuentes de evidencia independientes: como archivo reciente del sistema documentado en los archivos .lnk, como adjunto de correo electrónico enviado externamente mediante las comunicaciones documentadas en [CORR:1], y como tema de búsqueda implícito en el contexto de la navegación hacia PcComponentes. El hash SHA-256 del archivo adjunto es e6651b84f216a3575000b2352b4bc2c21490ca233abb4c430f14dde17e59cc9d.
[CORR:7]	HIGH	Secuencia temporal que vincula la creación o modificación de la cuenta personal de correo electrónico con las dificultades técnicas experimentadas durante los intentos de transmisión de documentación. El sistema de correo electrónico documentó una notificación de cambio de contraseña para la cuenta [redacted]lominguez[redacted]@gmail.com, recibida desde noreply@accounts.google.com, seguida inmediatamente por intercambios de correo electrónico entre el usuario [redacted] y [redacted] sobre problemas con el envío de documentación.

Línea Temporal de Eventos

La línea temporal establecida a partir de la evidencia disponible comprende diez eventos documentados, todos registrados con el timestamp preciso 2026-03-20T09:34:20.690676+00:00 que corresponde al momento de la adquisición forense del sistema. Este timestamp único para todos los eventos de acceso a archivos indica que el sistema operativo Windows registró estos accesos de forma simultánea, probablemente durante una operación de actualización del directorio de uso reciente triggered por la actividad del usuario momentos

antes de la adquisición.

Evento	**Descripción**
Descargas.lnk	Carpeta donde se almacenan los archivos recibidos a través del navegador o aplicaciones de red
general.lnk	Documento general cuyo nombre completo no fue preservado en los metadatos disponibles
impresion.lnk	Recursos de impresión del sistema
Internet.lnk	Configuraciones de conectividad de red
Listado de Proveedores.lnk	Información corporativa sensible sobre proveedores de la organización
Nuevo listado de Proveedores.lnk	Versión actualizada de información sobre proveedores
Política de uso aceptable - Spertas.lnk	Consulta deliberada de las políticas de seguridad corporativas
resultado de compras 2017.lnk	Documento posteriormente exfiltrado
Signatures.lnk	Configuraciones de firma digital o autenticación
timestamp de adquisición	09:34:20 UTC - establece el punto temporal máximo post quem para todos los eventos registrables

La correlación temporal establecida en [CORR:7] proporciona información sobre la secuencia de eventos que precedieron la adquisición, aunque sin timestamps absolutos para las comunicaciones de correo electrónico. La notificación de cambio de contraseña de Gmail y los intercambios subsiguientes sobre problemas de envío de documentación sugieren una secuencia donde el usuario experimentó dificultades técnicas al intentar transmitir archivos adjuntos corporativos, posiblemente relacionadas con restricciones de tamaño, formatos de archivo bloqueados, o limitaciones de las cuentas de correo configuradas.

El proceso de adquisición comenzó a las 09:21:49 UTC con el inicio de la colección de información del sistema y culminó a las 09:34:20 UTC con la finalización exitosa de todo el proceso. Los trece minutos transcurridos entre el inicio y la finalización de la adquisición representan el período durante el cual el sistema TRACIUM recopiló los diferentes módulos de información del sistema, desde la colección de información de hardware y red hasta la adquisición de artefactos de la papelera de reciclaje y el contenido del portapapeles.

Detalle de la Evidencia de Comunicaciones

Los hechos establecidos mediante el análisis de la evidencia corresponden exclusivamente a los datos contenidos en la imagen forense adquirida, sin incorporación de información externa no verificada. La evidencia de comunicaciones de correo electrónico documenta el envío del archivo resultado de compras 2017.xlsx desde la cuenta personal del usuario hacia [redacted] con el hash SHA-256 e6651b84f216a3575000b2352b4bc2c21490ca233abb4c430f14dde17e59cc9d que permite verificar la integridad del archivo transmitido. El contenido de los correos electrónicos incluye las expresiones textuales "Por fin he conseguido sortear los impedimentos técnicos que me impedían enviarte el documento de compras de 2017ƨ çualquier información relacionada con nuestro trato, mejor por correo personal", que evidencian directamente la intención de evadir los controles de seguridad corporativos.

La evidencia de artefactos de navegación web documenta las búsquedas realizadas desde el sistema bajo análisis, incluyendo consulta específica sobre cómo saltarse el firewall de la empresa mediante búsqueda en Google, consulta sobre cómo evadir filtros de contenido de Internet desde el trabajo publicada en computerhoy.com, búsqueda sobre cómo compartir archivos sin que los técnicos se enteren, e investigación sobre si un empresario puede bloquear las cuentas personales de un trabajador.

El historial de navegación también documenta visitas a sitios de distribuidores tecnológicos incluyendo Bechtle, PcComponentes, Megasur e Ingram Micro, así como búsquedas de productos HP en Amazon.es y el documento sobre vigilancia tecnológica IT. La evidencia del navegador web incluye la navegación hacia portableapps.com donde se localiza la página oficial de Mozilla Thunderbird Portable y la descarga subsiguiente del ejecutable portable.

Archivos de Acceso Directo Documentados

Los archivos de acceso directo .lnk documentados en la evidencia incluyen referencias a recursos del perfil de usuario [redacted]ocated en C:
Users
[redacted]
, específicamente en el directorio AppData
Roaming
Microsoft

Windows
Recent que Windows utiliza para almacenar accesos recientes. Los archivos .lnk preservados incluyen Descargas.lnk, general.lnk, impresion.lnk, Internet.lnk, Listado de Proveedores.lnk, Nuevo listado de Proveedores.lnk, Política de uso aceptable - [redacted]lnk, resultado de compras 2017.lnk y Signatures.lnk.

La presencia del archivo Política de uso aceptable - [redacted]lnk es particularmente relevante ya que indica que el usuario consultó deliberadamente las políticas de seguridad de la organización, evidenciando conocimiento de las normas que posteriormente habría violado.

Registros del Sistema

Los registros del sistema documentan dos cuentas de usuario configuradas en el sistema Windows bajo análisis, Admin con privilegios administrativos y [redacted]correspondiente al usuario bajo investigación. Los registros de seguridad indican que el sistema contaba con mecanismos de autenticación y control de acceso, aunque la evidencia sugiere que estos mecanismos fueron eludidos mediante el uso de cuentas legítimas por parte del propio usuario autorizado. Los registros de red documentan conexiones históricas del sistema hacia recursos externos, incluyendo servidores de correo electrónico, servidores DNS, y sitios web visitados durante las sesiones de navegación documentadas.

Limitaciones del Análisis

Las limitaciones técnicas del análisis realizado deben ser documentadas explícitamente para contextualizar adecuadamente el alcance válido de las conclusiones periciales.

El alcance temporal del análisis comprende exclusivamente el período de actividad registrable en la evidencia adquirida, estableciéndose como punto de referencia máximo la fecha y hora de adquisición de la imagen forense. Las actividades realizadas con posterioridad a la adquisición no están disponibles para análisis, y la evidencia de actividades anteriores debe ser inferida a partir de los artefactos creados o modificados durante estas actividades, lo que introduce incertidumbre sobre la secuencia exacta de eventos y los intervalos temporales entre ellos.

La evidencia analizada corresponde exclusivamente a un sistema endpoint Windows sin acceso a otros componentes de la infraestructura corporativa. Los servidores de correo

electrónico de la organización, los sistemas de monitorización de red perimetral, los dispositivos de seguridad perimetral como firewalls y sistemas de prevención de intrusiones, y otros endpoints del mismo usuario no han sido acquiredos para análisis. Esta limitación significa que las comunicaciones de correo electrónico documentadas representan únicamente las copias locales almacenadas en el sistema bajo análisis, sin que se hayan podido verificar en los servidores corporativos o externos correspondientes. Las conexiones de red documentadas se limitan a los registros disponibles en el sistema local, sin acceso a logs de servidores proxy, firewalls o sistemas de detección de intrusiones que pudieran proporcionar visibilidad completa del tráfico de red.

La adquisición forense mediante el sistema TRACIUM capturó los artefactos presentes en el sistema en el momento de la adquisición, pero no garantiza la captura exhaustiva de todos los datos relevantes. Las aplicaciones configuradas en modo de navegación privada o las comunicaciones realizadas mediante servicios web podrían no haber dejado rastro en los artefactos acquisicionados. La eliminación intencional de artefactos por parte del usuario antes de la adquisición representaría una limitación adicional que no puede ser verificada mediante los datos disponibles. Los archivos eliminados que no fueron sobrescritos podrían haber sido recuperados mediante técnicas de análisis forense de almacenamiento, aunque la metodología de adquisición aplicada no incluyó la extracción de espacio no asignado o la búsqueda de archivos eliminados en áreas libres del sistema de archivos.

La ausencia de ciertos tipos de artefactos en la evidencia disponible no permite descartar la existencia de actividades que pudieran haber dejado rastro exclusivamente en sistemas no acquiredos o que hubieran sido eliminadas antes de la adquisición. Las búsquedas web documentadas proporcionan evidencia de la premeditación de las actividades de evasión, pero la ausencia de timestamps específicos para estas búsquedas limita la capacidad de establecer la secuencia cronológica precisa entre la planificación y la ejecución de las actividades de exfiltración. Las comunicaciones de correo electrónico documentadas indican el resultado de las actividades de transmisión, pero la evidencia no incluye necesariamente todas las comunicaciones relevantes que pudieran haber existido durante el período de actividad del usuario.

Los registros de cadena de custodia documentan la preservación e integridad de la evidencia adquirida, pero la calidad de los hallazgos depende directamente de la calidad y completitud de la evidencia source. Los valores hash criptográficos documentados permiten verificar que los artefactos analizados no han sido modificados desde su adquisición, pero no pueden compensar la ausencia de datos que nunca fueron creados o que fueron eliminados antes de la adquisición. La interpretación de los hallazgos debe considerar estas limitaciones reconocidas, evitando conclusiones que excedan el alcance de la evidencia

disponible o que se basen en inferencias no sustentadas en los datos documentados.

4. Conclusiones

El análisis forense de la evidencia identificada como [EVID:1] ha permitido establecer, con alto grado de certeza técnica basado en las correlaciones documentadas, que el usuario [redacted] del sistema **Windows** bajo análisis realizó actividades deliberadas de exfiltración de datos corporativos y evasión intencional de los controles de seguridad implementados por [redacted] Esta conclusión se fundamenta en la convergencia de múltiples fuentes de evidencia independientes que configuran un escenario forense coherente y concluyente [CORR:1][CORR:4].

Las comunicaciones de correo electrónico analizadas proporcionan evidencia directa de la transmisión no autorizada de información corporativa confidencial al tercero externo [redacted] El contenido del correo electrónico enviado desde la cuenta personal [redacted]**@gmail.com** incluye expresiones textuales que evidencian claramente la intención deliberada de sortear los impedimentos técnicos establecidos por la organización, específicamente la frase donde el usuario manifiesta haber conseguido evadir las restricciones que le impedían transmitir el documento de compras de 2017. El archivo adjunto identificado como resultado de compras 2017.xlsx presenta el hash **SHA-256** e6651b84f216a3575000b2352b4bc2c21490ca233abb4c430f14dde17e59cc9d que permite verificar la integridad del archivo transmitido [CORR:1][CORR:6].

El historial de navegación web documenta búsquedas deliberadas que evidencian la premeditación de las actividades de evasión de seguridad. El usuario consultó términos específicos orientados a:

- Conocer cómo sortear **firewalls** corporativos
- Cómo evadir **filtros de contenido de Internet** desde el trabajo
- Cómo compartir archivos sin que el departamento de tecnologías de la información tuviera conocimiento
- Si un empresario podía bloquear las cuentas personales de un trabajador

Estas búsquedas demuestran que el usuario planificó sus acciones de evasión antes de ejecutarlas, refuerzando la conclusión de intencionalidad deliberada en las violaciones documentadas [CORR:2].

La descarga e instalación de **Mozilla Thunderbird Portable** en el sistema constituye el método técnico específico utilizado para establecer canales de comunicación no

monitorizados. El ejecutable **ThunderbirdPortable_60.3.0_English.paf.exe** fue obtenido desde **portableapps.com** y configurado para gestionar tanto la cuenta corporativa como la cuenta personal del usuario. La naturaleza **portable** de esta aplicación, que no requiere instalación formal en el sistema operativo, evadió los inventarios de software monitorizados por el departamento de tecnologías de la información, permitiendo al usuario mantener comunicaciones paralelas fuera de los controles de seguridad corporativos [CORR:3].

La evidencia de acceso a documentos corporativos confidenciales queda documentada mediante los archivos de acceso directo **Windows .lnk** presentes en el perfil de usuario. El sistema registró accesos a:

- resultado de compras 2017.lnk
- Listado de Proveedores.lnk
- Nuevo listado de Proveedores.lnk
- **Política de uso aceptable -** [redacted] **lnk** (de manera especialmente relevante)

Esto demuestra que el usuario consultó deliberadamente las políticas de seguridad de la organización, evidenciando su conocimiento de las normas que posteriormente violó con las actividades documentadas [CORR:4][CORR:6].

El usuario [redacted] es identificado como actor activo principal del sistema mediante los registros del sistema operativo, que documentan dos cuentas configuradas, **Admin** con privilegios administrativos y [redacted] con privilegios de usuario estándar. Las comunicaciones de correo electrónico identificadas conectan las cuentas corporativas **julian**[redacted]**info** y personal [redacted]**@gmail.com** con este usuario específico, estableciendo la atribución inequívoca de todas las actividades documentadas [CORR:4].

Las actividades identificadas constituyen vulneraciones claras de las políticas internas de uso aceptable de [redacted]

- El acceso no autorizado a información corporativa confidencial
- La transmisión de dicha información a terceros externos sin autorización
- El uso de software no autorizado para evadir controles de seguridad

- La utilización de cuentas de correo personales para ocultar comunicaciones del departamento de tecnologías de la información

La consulta deliberada de la política de uso aceptable documentada en los archivos .lnk demuestra el conocimiento del usuario sobre las normas violadas.

El perfil de amenaza identificado corresponde a un incidente de seguridad de origen interno con intencionalidad claramente maliciosa, donde un usuario legítimo del sistema utilizó sus credenciales y acceso autorizado para realizar actividades que violan las políticas corporativas y que potencialmente constituyen delitos bajo la legislación aplicable. Las siete correlaciones de alta y media prioridad identificadas configuran un escenario forense que demuestra con alto grado de certeza técnica la existencia de este incidente.

Las limitaciones reconocidas del análisis se circunscriben al alcance de la evidencia disponible, correspondiente exclusivamente a un sistema endpoint **Windows** sin acceso a infraestructura de red corporativa, servidores de correo electrónico o sistemas de monitorización de seguridad. Sin embargo, estas limitaciones no afectan la validez de las conclusiones alcanzadas, ya que las evidencias documentadas son suficientemente concluyentes para establecer los hechos del caso y sustentar las acciones que la organización considere apropiadas.

5. Anexos

ANEXO I: CADENA DE CUSTODIA

Registros de verificación de integridad, cambios de custodia y operaciones realizadas durante el proceso de adquisición forense mediante el sistema TRACIUM.

Timestamp	**Source**	**Nivel**	**Mensaje**
2026-03-20 09:21:49	TRACIUM	INFO	Starting complete system acquisition process
2026-03-20 09:21:49	TRACIUM	INFO	Starting system information collection
2026-03-20 09:21:50	TRACIUM	INFO	Starting network information collection
2026-03-20 09:21:50	TRACIUM	INFO	Starting hardware information collection
2026-03-20 09:21:50	TRACIUM	INFO	Network information collection completed successfully
2026-03-20 09:21:50	TRACIUM	INFO	Hardware information collection completed successfully
2026-03-20 09:21:50	TRACIUM	INFO	Starting security information collection
2026-03-20 09:21:51	TRACIUM	INFO	Starting browser artifacts collection
2026-03-20 09:21:51	TRACIUM	INFO	Security information collection completed successfully
2026-03-20 09:21:51	TRACIUM	INFO	Starting forensics data collection
2026-03-20 09:30:19	TRACIUM	INFO	Collecting communication artifacts
2026-03-20 09:31:39	TRACIUM	INFO	Collecting recent files
2026-03-20 09:31:41	TRACIUM	INFO	Collecting command history
2026-03-20 09:31:42	TRACIUM	INFO	Collecting scheduled tasks
2026-03-20 09:31:42	TRACIUM	INFO	Collecting system logs
2026-03-20 09:31:42	TRACIUM	INFO	Collecting network history
2026-03-20 09:34:07	TRACIUM	INFO	Collecting active connections
2026-03-20 09:34:07	TRACIUM	INFO	Collecting SSH keys
2026-03-20 09:34:07	TRACIUM	INFO	Collecting hosts file
2026-03-20 09:34:08	TRACIUM	INFO	Collecting installed software
2026-03-20 09:34:09	TRACIUM	INFO	Collecting recent downloads
2026-03-20 09:34:09	TRACIUM	INFO	Collecting environment variables
2026-03-20 09:34:11	TRACIUM	INFO	Collecting USB history
2026-03-20 09:34:11	TRACIUM	INFO	Collecting prefetch files
2026-03-20 09:34:12	TRACIUM	INFO	Collecting clipboard content
2026-03-20 09:34:12	TRACIUM	INFO	Collecting recycle bin

Timestamp	Source	Nivel	Mensaje
2026-03-20 09:34:12	TRACIUM	INFO	Forensics data collection completed successfully
2026-03-20 09:34:19	TRACIUM	INFO	Complete system acquisition process finished successfully

Total de entradas documentadas: 29

ANEXO II: LÍNEA TEMPORAL DE EVENTOS

Eventos del sistema registrados durante la adquisición forense, incluyendo accesos a archivos documentados en el perfil de usuario [redacted]

Timestamp	**Source**	**Tipo de Evento**	**Descripción**
2026-03-20 09:34:20.690676+00:00	tracium	system_collection	System data collected from tracium_1773999260_1773999260690675633
2026-03-20 09:34:20.690676+00:00	tracium	file_access	File accessed: Descargas.lnk
2026-03-20 09:34:20.690676+00:00	tracium	file_access	File accessed: general.lnk
2026-03-20 09:34:20.690676+00:00	tracium	file_access	File accessed: impresion.lnk
2026-03-20 09:34:20.690676+00:00	tracium	file_access	File accessed: Internet.lnk
2026-03-20 09:34:20.690676+00:00	tracium	file_access	File accessed: Listado de Proveedores.lnk
2026-03-20 09:34:20.690676+00:00	tracium	file_access	File accessed: Nuevo listado de Proveedores.lnk
2026-03-20 09:34:20.690676+00:00	tracium	file_access	File accessed: Politica de uso aceptable - [redacted]lnk
2026-03-20 09:34:20.690676+00:00	tracium	file_access	File accessed: resultado de compras 2017.lnk
2026-03-20 09:34:20.690676+00:00	tracium	file_access	File accessed: Signatures.lnk

Total de eventos documentados: 10

ANEXO III: CORRELACIONES IDENTIFICADAS

Relaciones establecidas mediante análisis de inteligencia artificial entre las diferentes fuentes de evidencia, clasificadas por tipo y nivel de confianza.

Correlación	Tipo	Descripción	Confianza
[CORR:1]	CAUSAL	Comunicación de correo electrónico documenta el envío del archivo resultado de compras 2017.xlsx desde la cuenta personal del usuario[redacted]n-guez hacia[redacted] El contenido evidencia la intención de sortear controles de seguridad corporativos y solicitar uso de correo personal para evitar detección.	HIGH
[CORR:2]	USER	Historial de navegación muestra búsquedas deliberadas para evadir controles de seguridad de la empresa, incluyendo consultas sobre cómo sortear firewalls, filtros de Internet, compartir archivos sin conocimiento de técnicos, y capacidades del empleador para bloquear cuentas personales.	HIGH
[CORR:3]	CAUSAL	Usuario descargó Thunderbird Portable, una aplicación portable de correo electrónico que permite establecer canales de comunicación no monitorizados evadiendo inventarios de software corporativos.	HIGH
[CORR:4]	USER	Sistema identifica al usuario[redacted]como actor activo principal del sistema. Las cuentas corporativas y personales del usuario se conectan con las comunicaciones externas documentadas.	HIGH
[CORR:5]	CUSTOM	Historial de navegación muestra investigación sobre distribuidores de tecnología incluyendo Bechtle, PcComponentes, Megasur e Ingram Micro, correlacionando con comunicaciones sobre compras con otros proveedores.	MEDIUM
[CORR:6]	TEMPORAL	El documento resultado de compras 2017.xlsx aparece en múltiples fuentes de evidencia independientes: archivo reciente del sistema, adjunto de correo electrónico enviado externamente, y tema de búsqueda en navegador.	HIGH

Correlación	Tipo	Descripción	Confianza
[CORR:7]	TEMPORAL	Notificación de cambio de contraseña de cuenta Gmail personal seguida inmediatamente por intercambios de correo sobre problemas con envío de documentación.	HIGH

Total de correlaciones identificadas: 7

ANEXO IV: INVENTARIO DE EVIDENCIAS ANALIZADAS

Relación de evidencias digitales analizadas durante el proceso de correlación, con identificadores únicos, tipo de fuente y contenido.

ID	Tipo	Contenido
[EVID:1]	tracium	Evidencia principal del caso. Imagen forense del disco duro de estación de trabajo Windows. Hash de evidencia no especificado en los datos disponibles.
[EVID:2]	tracium	Email: Re Envío de documento [redacted] From: [redacted]m-guez [redacted]@gmail.com, To: [redacted]@companyexample.com. Body menciona compras puntuales con otros proveedores y preferencia por correo personal.
[EVID:3]	tracium	Email: Envío de documento [redacted] From: [redacted] [redacted]@gmail.com, To: [redacted]@companyexample.com. Attachment IDs: resultado de compras 2017.xlsx. Body menciona haber sortear impedimentos técnicos.
[EVID:4]	evidex	Attachment: 1_resultado de compras 2017.xlsx. Hash SHA-256: e6651b84f216a3575000b2352b4bc2c21490ca233abb4c430f14dde17e59cc9d
[EVID:5]	tracium	Browser History: como saltarse el firewall de la empresa. URL: https://www.google.com/search?q=c%25C3%25B3mo+saltarse+el+firewall+de+la+empresa
[EVID:6]	tracium	Browser History: Como saltarse el filtro de Internet desde el trabajo. URL: https://computerhoy.com/paso-a-paso/life/como-saltarse-filtro-internet-trabajo-22825
[EVID:7]	tracium	Browser History: compartir archivos sin que los técnicos se enteren. URL: Google search
[EVID:8]	tracium	Browser History: puede un empresario bloquear las cuentas personales de un trabajador. URL: Google search
[EVID:9]	tracium	Browser History: thunerbird portable. URL: https://www.google.com/search?q=thunerbird+portable
[EVID:10]	tracium	Browser History: Mozilla Thunderbird Portable. URL: https://portableapps.com/apps/internet/thunderbird_portable

ID	Tipo	Contenido
[EVID:11]	tracium	Browser History: ThunderbirdPortable_60.3.0_English.paf.exe. URL: http://download3.portableapps.com/portableapps/ThunderbirdPortable/ThunderbirdPortable_60.3.0_English.paf.exe
[EVID:12]	tracium	Users: Admin, [redacted]
[EVID:13]	tracium	Email: RE Felicidades y presentación. From: [redacted] Dominguez [redacted] info, To: [redacted] @companyexample.com
[EVID:14]	tracium	Email: Felicidades y presentación. From: [redacted] @companyexample.com, To: [redacted] julian [redacted] info
[EVID:15]	tracium	Browser History: documento it surviallance. URL: Google search
[EVID:16]	tracium	Browser History: mejores distribudores de informatica espana. URL: https://www.google.es
[EVID:17]	tracium	Browser History: http://www.bechtle.es/
[EVID:18]	tracium	Browser History: Amazon.es servidor hp. URL: Amazon.es
[EVID:19]	tracium	Browser History: http://www.pccomponentes.com/
[EVID:20]	tracium	Recent File: resultado de compras 2017.lnk. Path: C:\Users\[redacted]\AppData\Roaming\Microsoft\Windows\Recent\resultado de compras 2017.lnk
[EVID:21]	tracium	Email: Se ha modificado la contraseña. From: Google no-reply@accounts.google.com, To: [redacted] pertas@gmail.com
[EVID:22]	tracium	Email: Problemas con envío de documentación. From: [redacted] info, To: [redacted] @companyexample.com
[EVID:23]	tracium	Email: Re Problemas con envío de documentación. From: [redacted] @companyexample.com, To: [redacted] Dominguez [redacted] info

Total de evidencias inventariadas: 23

Declaración de independencia

El/la perito/a firmante declara que el presente informe ha sido elaborado conforme a su leal saber y entender, con rigor técnico, independencia y objetividad, y que no mantiene relación alguna con las partes implicadas en el procedimiento que pueda comprometer su criterio técnico.

Firma del perito:

Perito Informático Certificado
Certificado en Informática Forense y Análisis de Sistemas
Fecha: 20 de marzo de 2026